



Procedures for Reporting ARIES Security Incidents

All ARIES users are required to take **all** necessary steps to protect the confidentiality and security of the Protected Health Information (PHI) entered and stored in ARIES.

Examples of PHI contained in ARIES are as follows (includes Related/Affected Clients):

Client Name	Client Address
Client Telephone Numbers	Client Fax Numbers
Client E-mail addresses	Client Medical Record Number
Social Security Number	Date of Birth
Health Plan Beneficiary Number	Account Numbers
Client's Mother's Maiden Name	Client's Family Member's Name
Unencrypted Unique Record Number (URN)	

Provider staff need to be aware of and follow their agency's guidelines pertaining to patient confidentiality and the Health Insurance Portability and Accountability Act (HIPAA).

Additionally, staff and agencies are required to report any breaches of security pertaining to PHI. A breach is defined as any failure to follow confidentiality protocols and procedures, ***whether or not PHI is actually released***. The nature of the security breach—whether PHI was actually released or not—determines who to report the breach to and the timing required:

- Security incidents which ***do not release*** PHI should be reported to agency management as soon as possible (usually a person's direct supervisor).
- The incidents that ***do release*** PHI must be ***immediately*** reported to (1) your agency management, (2) your County Health Department and/or Ryan White Part A Grantee (if your agency receives funds from these entities), and (3) the California Department of Health Services, Office of AIDS (CDHS/OA).

Examples of security breaches that do ***not*** release PHI which should be reported to agency management are as follows: a compromised ARIES password, noticing that another staff person has posted their ARIES login and password where others can see it, staff walking away from their computer monitors with client information in view, ARIES-generated reports with PHI available where other staff can see them, etc.

Examples of breaches that ***do*** release PHI which need to be reported to your County/Grantee ***and*** the CDHS/OA are as follows: accidental or intentional release of client information to the public or staff who have no business need to see the information (e.g., e-mailing a report with client names and addresses to staff outside your agency), inappropriate use of ARIES (e.g., users looking for ARIES information on acquaintances, friends, family, etc.), stolen or lost computer which was used to access ARIES (that might contain copies of ARIES reports with PHI), etc.



Procedures for Reporting ARIES Security Incidents

To report a security incident to the CDHS/OA, call Susan Sabatier at (916) 449-5844 or the ARIES System Administrator at (916) 449-5842. If you are unable to contact a person, leave a voicemail message and also send a brief e-mail regarding the incident to aries@dhs.ca.gov.

Depending upon the seriousness of the security incident, CDHS/OA may also report the incident to the CDHS Security Officer.

Breaches will be appropriately investigated to determine causes and implement corrections. Additionally, any and all sanctions, as specified by contracts and/or State and Federal law will be enforced.

For questions or clarifications regarding the reporting of ARIES security incidents, contact your Part A Grantee's ARIES lead or Susan Sabatier, CDHS/OA at ssabatie@dhs.ca.gov.